http://www.airpower.au.af.mil/home.htm

It's Time to Fight Back

"Operationalizing" Network Defense

Mr. Nicolas Adam Fraser
Lt Col Robert J. Kaufman III, USAF, Retired
Lt Col Mark R. Rydell, USAF, Retired*

The Air Force's decision to stand up Twenty-fourth Air Force under Air Force Space Command creates an opportunity to scrutinize existing network warfare constructs with the goal of ensuring that network warfare operations carry out the Air Force's stated mission: "to fly, fight, and win . . . in air, space, and cyberspace."[1] Such a sweeping review would involve a significant number of organizations inside and outside the Air Force, encompassing discussions of policy, funding priorities, personnel, and cross-service coordination, to name a few. This article does not attempt to address all of the complex issues surrounding cyberspace operations; rather, it examines the most visible component of cyberspace warfare—network defense (NetD).

Since 1992 the Air Force has monitored its networks and responded to malicious network events. As the service has matured its ability to command and control its networks, some operational principles have unintentionally blended NetD and network operations (NetOps). This article proposes new operational constructs that will force a healthy distinction between network warfare—particularly NetD—and NetOps. Cyber targeting, the first proposed construct, emphasizes the need to proactively find, fix, track, and target an adversary. Cyber targeting operations can ensure that mission-critical systems or even network paths remain free of adversaries. The second construct, cyber engagement, is a collection of responses specifically designed to affect an identified intruder. Current NetD constructs and cyber targeting enable cyber engagement operations. Finally, we must closely coordinate both targeting and engagement operations with combatant commands (COCOM) and other national agency operations. Both cyber targeting and cyber engagement induce a robust contrast between maintenance of the network and defense of the network. Making such a distinction and employing the proposed constructs should result in more effective NetD operations.

Setting the Stage for Change

The Air Force has been discriminating in its definitions of NetOps and NetD, the former providing "effective, efficient, secure, and reliable information network services used in critical Department of Defense (DOD) and Air Force communications and information processes" and the latter "employ[ing] . . . network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt,

*All three authors work at the 688th Information Operations Wing at Lackland AFB, Texas, Mr. Fraser as chief of the Network Access Engineering Branch, Lieutenant Colonel Kaufman as deputy director of the 318th Information Operations Group, and Lieutenant Colonel Rydell as a senior associate with Booz, Allen, and Hamilton. All served tours on the Air Force Computer Emergency Response Team.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
It's Time to Fight Back: 'Operationalizing' Network Defense	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **688th Information Operations Wing,Lackland AFB,TX,78236**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

or usurp it. NetD can be viewed as planning, directing, and executing actions to prevent unauthorized activity in defense of Air Force information systems and networks and for planning, directing, and executing responses to recover from unauthorized activity should it occur."[2] The fact that the joint community does not have a term to describe what the Air Force calls NetOps means that it considers NetOps either a subset of NetD or simply a maintenance function that does not warrant discussion in a joint doctrine publication.[3] Due to the differences in joint and Air Force doctrine, we suggest simplified versions of NetD and NetOps so that the reader can immediately recognize each operation's responsibilities and priorities:

- network warfare operations / NetD: operations that seek to produce desired effects against an adversary tactically, operationally, and strategically. These operations, which require planning and intelligence support, can be reactive or proactive. Most importantly, NetD operations consider the discovery of an adversary not just a threat but an opportunity for operational engagement.
- NetOps: operations in which the maintainer primarily *acts upon the network* to provide reliable and secure network services. In reality an adversary who disrupts operations is no worse than a hardware failure since the goal involves maintaining availability and performance requirements. Just as we can replace hardware, so can we rebuild a compromised computer.

We contend that the Air Force does not actually conduct NetD operations as defined above. We support this claim by examining two principles that lie at the core of the service's current approach to NetD and that keep the Air Force reactive, thus weakening its ability to defend the network effectively.

Principle 1: Detecting the Adversary Is Paramount

This principle, the foundation upon which we have built most traditional NetD, consumes the bulk of the Air Force's NetD resources. The service relies on real-time monitoring and emphasizes hardened network perimeters to detect enemy activity. However, its motivation for doing so is of great importance. The Air Force wishes to detect the intruder or attacker, not to take action against him but to find and fix a security problem. The situation is analogous to how a security forces member on flightline patrol responds to a suspicious event. Upon seeing an intruder enter through a hole in the fence, he or she shines his flashlight on the hole and begins to fix it instead of following and capturing the intruder. Currently the Air Force makes no distinction between sophisticated and nonsophisticated intrusions, treating all breaches equally and responding in a way that protects and reestablishes the health of the network. It does not focus on assuring that we can perform required missions and continue NetOps despite adversary attacks.

Though important, detecting the adversary is not the only way to protect a network. Rapidly and regularly changing its configuration would also offer protection and would not require detection of the adversary to produce results.[4] Additionally, we do not advocate the end of detection efforts, something critical to NetD operations as we define it, but the motivation behind detection efforts must change. Finally, we concede that our best perimeter defenses and patch-management methodologies fail to deter or hinder sophisticated adversaries.[5] Although these methodologies are useful, we must supplement our current approach with one committed to achieving effects against the adversary and assuring mission success.

Principle 2: NetD Operations Are Successful When a Compromised Computer Is No Longer Compromised

This principle relegates NetD operations to a maintenance role within the Air Force, emphasizing network health at the expense of determining the enemy's effect on ongoing or future missions. Furthermore, we rarely use a compromised computer to engage the adversary. In addition to finding, analyzing, and fixing compromised computers, NetD operators must contest the adversary, even on our own networks, conceiving of and executing defensive strategies that affect him while assuring the integrity of priority war-fighting missions.

Because of this principle, probably more than its companion, we should really define the current NetD as NetOps. When an intrusion occurs and we open an "incident," when do we close it? Not when an operation concludes but when we consider the computer free of intruders and allow it to rejoin the network. Is that success? No. We should measure success by combat effectiveness; consequently, we must take measurements at the strategic, operational, and tactical levels to determine if we are attaining NetD objectives such as deterring the adversary from establishing or employing offensive capabilities against US interests.[6]

A New Construct

We propose correcting these problems by establishing operational units (of yet undetermined sizes) charged with truly affecting adversary operations that target Air Force and DOD networks. True, units in Twenty-fourth Air Force (including the 688th Information Operations Wing and the 67th Network Warfare Wing) are responsible for executing the Air Force's cyber mission; however, no units within Twenty-fourth Air Force now do what we suggest below. Our new paradigms will require reshaping existing units and, possibly, creating new ones.

The first proposed organization would have the inwardly focused mission of seeking out the adversary on Air Force and DOD networks. The second would have the outwardly focused mission of engaging him on those networks. Although both would work closely together (and with the established, continuous network-monitoring mission), they would be set apart by their commitment to planned missions or "sorties" linked to a commander's operational needs and terminated upon completion of the mission. At strategic levels, proper policies need to endorse proactive NetD strategies such as targeting and engagement. Next, at the operational level, we must develop plans to address specific adversaries and prescribe approved courses of action that allow network defenders to realize unity of effort, mass, surprise, and timeliness in cyberspace. Finally, at the tactical level, we must train and certify operators on NetD weapons that can compromise attacks or thwart attempts to gain access to Air Force networks. These organizations and plans will allow the Air Force to perform NetD operations that seek, engage, and act upon adversaries in cyberspace.

Cyber Targeting

Clearly, enemies—specifically advanced, persistent ones—reside within the Air Force network. Spearfishing attacks, which persuade users either to open a malicious attachment or click on a link to a malicious Web page, breach perimeter defenses without difficulty. The ease with which an adversary can gain access to DOD networks is outdone only by the ease with which he can navigate and maneuver after establishing "beachheads" within Air Force and DOD networks, both of which actions offer entry to high-value information or systems. A proactive approach, cyber targeting can identify intruders on our networks by using state-of-the-art NetD "weapons" not permanently located on the Air Force network, along with typical perimeter-security tools. We would conduct operations with a specific objective in mind, find the adversary, and then influence, disrupt,

or otherwise affect him. An operation would not terminate until we have identified the adversary and subsequently verified his absence, regardless of the terminating factor. These operations also demand proper planning and execution because of the tremendous amount of legitimate data in cyberspace, within which the adversary hides to do his work.

Cyber Engagement

Defense has always involved delaying, disrupting, deterring, or denying enemy objectives. However, if we assume the impossibility of completely stopping the adversary, then we must consider ways to significantly hinder or exploit his efforts. (By "exploit," we mean achieve second- and third-order effects on his decision-making capacity.) Cyber engagement makes the conscious decision to use DOD networks as a path to the adversary—a path for fulfilling defensive goals.[7] Upon discovering a compromised computer or network, NetD operators no longer would simply rebuild the system but would use intelligence and perhaps other NetD weapons to identify the intruder. Next, depending on the level of attribution and existing operation plans (OPLAN), they would conduct tactical operations against the adversary, utilizing the compromised computer or network as a launching point.[8] For example, during an operation, the NetD operator could intentionally pass inaccurate information to the enemy or manipulate exfiltrated data, rendering it untrustworthy. Regardless of the technique employed, the operator would always try to introduce unreliability, make intrusions more costly, or influence the adversary's actions. Consequently, operators must plan and coordinate these "response actions" with larger COCOM or national-level strategies.[9] Additionally, they must deconflict these kinds of operations from the day-to-day monitoring of network sensors.

As discussed above, cyber engagement covers a spectrum of operations, not simply network attack. Engagement assumes the inability of detection and protection efforts to defend the network properly. Instead it takes a different approach, one not limited to selection of a particular technology but concerned with actions necessary to meet defensive goals. To illustrate, during a football game, the offensive players attempt to reach the end zone, but the defense tries to stop them. Football defenses attempt to keep the opposing team out of the end zone not only by employing defense in depth (fielding a strong defensive line, linebackers, and safeties) but also by using different schemes to confuse the quarterback. For example, one linebacker might rush the quarterback while two others drop back in coverage—or the defensive coordinator might call for an all-out blitz. Regardless of the scheme, good coaches know they cannot always prevent the offense from scoring, but they can make its task difficult by confusing the opposing players, especially the quarterback.

With one eye on this analogy, we would have to say that the DOD currently plays defense without ever thinking about causing confusion amongst the offense. We don't have different defensive schemes, nor do we prepare plans for affecting the planning, execution, and, ultimately, the outcome of an encounter with the enemy. Instead our defense stands at the network perimeter, and we hope no one gets by undetected.

Cyber targeting and cyber engagement represent a significant paradigm shift in the way we conduct NetD operations. By factoring in the objectives of focused OPLANs, we can make NetD a stronger form of fighting than network attack.[10] Indeed, the US Army has already noted this in more traditional defensive operations.[11] Furthermore, NetD can take a more active role in network warfare while creating a much-needed distinction between itself and NetOps. Finally, these new constructs support the president's desire to go beyond criminal prosecution in responding appropriately to cyber attacks.[12]

A Simple Proposal

Planning and preparing for large-scale military operations, such as the invasion of Iraq in 2003, require that COCOM OPLANs be routed through each military service's lead NetD organization, thereby allowing network defenders to implement measures against enemy targeting of DOD networks and prevent any disruption of the OPLAN's execution. Requirements provided by the COCOMs usually address generic threats. When operations commence, we usually take proactive steps such as blocking the addresses of hostile Internet protocols.

In these traditional situations, we treat the networks as a support element. That is, our networks need to function without disruption in order for our symmetric warfare capabilities to operate—analogous to saying that the fuel trucks need to function so the F-16s can take off. It is difficult to contemplate fighting on US networks, but NetD operations must take advantage of access to enemy NetOps and respond by decreasing the credibility of stolen information, increasing the cost of an attack on Air Force and DOD networks, or allowing the United States to influence the adversary's perceptions prior to and during all phases of conflict.

We propose the following as a way of highlighting the utility of this new construct, which truly thinks of NetD as a form of asymmetric warfare. Currently, each OPLAN has an appendix that addresses NetD requirements. However, in addition to providing for preventive network protection, future OPLANs should identify the systems critical to performing traditional warfare operations (e.g., logistics networks, command and control nodes, etc.). Moreover, we should pinpoint high-threat adversaries so we can begin planning and coordinating cyber engagement operations, and we should plan and execute targeting operations on mission-critical systems identified by the COCOM. However, this time if we discover the adversary, we should commence engagement operations to affect or influence him.

Two important points merit emphasis. First, the adversary discovered during targeting operations might be entirely different from the one addressed by the OPLAN—a possibility that makes cyberspace such a challenging domain to dominate. Second, targeting and engagement operations do not necessarily have to be linked to a specific COCOM OPLAN. We can perform proactive targeting operations as long as we properly delineate and synchronize them with other operations. We should consider performing engagement operations every time we discover a network intrusion, whether through traditional detection techniques or targeting operations.

Conclusion

According to the 67th Network Warfare Wing, "The bottom line is that the Air Force must transition from a detection-centric orientation to an active network kill chain approach which integrates prevention, detection, response, and adversary engagement."[13] This vision cannot come to fruition without organizing and tasking NetD operational units to change their operational constructs from a reactive approach (monitor, detect, and respond) to one that, as recently described by Lt Gen William T. Lord, "seek[s] out threats and . . . detect[s] and defeat[s] them instantaneously."[14] We cannot do this in isolation. We need purposeful planning and coordination with intelligence and national-level agencies. Furthermore, the creation of US Cyber Command should help ensure that services act under the authority and direction of a COCOM. The cyber targeting and cyber engagement constructs truly "operationalize" NetD since they focus squarely on acting upon and affecting the adversary. In the future, we should pay comparable attention to mission assurance (i.e., continuing operations despite enemy attacks), an area that prevents the complete separation of

NetD and NetOps. However, we cannot adequately address it without planning and very good intelligence. The DOD spends $100 million every six months to defend the .mil network.[15] At some point, we must ask ourselves whether we are reaching our defensive goals and deterring adversaries. Today, we are not, but by operationalizing NetD and concentrating on affecting the enemy, we can reverse this trend so that the Air Force can fight back. ✪

Lackland AFB, Texas

Notes

1. Air Force Program Action Directive 07-08, *Phase One of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces*, 19 December 2008, 8.

2. Air Force Instruction 33-115, vol. 1, *Network Operations (NETOPS)*, 24 May 2006, 3, http://www.af.mil/shared/media/epubs/AFI33-115V1.pdf (accessed 13 May 2010); and Air Force Doctrine Document 2-5, *Information Operations*, 11 January 2005, 20, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5.pdf (accessed 13 May 2010).

3. Joint Publication 3-13, *Information Operations*, 13 February 2006, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 13 May 2010).

4. Spyros Antonatos et al., "Defending against Hitlist Worms Using Network Address Space Randomization," *Computer Networks* 51, no. 12 (22 August 2007): 3471–3490; and Dorene Kewley et al., "Dynamic Approaches to Thwart Adversary Intelligence Gathering," in *Proceedings of the DARPA [Defense Advanced Research Projects Agency] Information Survivability Conference and Exposition*, vol. 1 (2001), 176.

5. "Engaging the Adversary on Air Force Networks," Information Assurance Technology Analysis Center Report, TAT 04-25, DO 232, 5 March 2007, 1.

6. Chairman, Joint Chiefs of Staff, to distribution list, memorandum, subject: National Military Strategy for Cyberspace Operations (without enclosure), December 2006, 13, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 14 May 2010).

7. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 87.

8. *Attribution* means the degree of confidence with which we can identify the adversary.

9. John P. Stenbit, assistant secretary of defense for command, control, communications, and intelligence, to secretaries of the military departments et al., memorandum, subject: Guidance for Computer Network Defense Response Actions, 26 February 2003, https://powhatan.iiie.disa.mil/cnd/cnd-ra-matrixand-memo.pdf (accessed 14 May 2010).

10. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 84.

11. Field Manual 3-01.7, *Air Defense Artillery Brigade Operations*, 31 October 2000, 6-36, http://www.theblackvault.com/documents/fm3_01x7.pdf (accessed 14 May 2010).

12. White House, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, February 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed 14 May 2010) .

13. 26th Network Operations Group, "NetD Concept of Employment," final draft, 14 December 2007, 2.

14. Chuck Paone, "General Calls for New Thinking on Cyberspace," 12 May 2009, http://www.af.mil/news/story.asp?id=123148876 (accessed 8 April 2010).

15. William Jackson and Doug Beizer, "New DOD Cyber Command Will Focus on the Dot-Mil Domain," *Government Computer News*, 15 June 2009, http://gcn.com/Articles/2009/06/15/Web-DOD-cyber-command.aspx?p=1 (accessed 8 April 2010).